

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK**

RONALD JANTZER, on behalf of himself
and all others similarly situated,

Plaintiff,

8:19-cv-00791 (BKS/DJS)

v.

ELIZABETHTOWN COMMUNITY HOSPITAL,
and UNIVERSITY OF VERMONT HEALTH
NETWORK INC.,

Defendants.

Appearances:

For Plaintiff:

Brian P. Murray
Glancy Prongay & Murray LLP
230 Park Avenue, Suite 530
New York, NY 10169

Jean S. Martin
John Y. Yanchunis
Morgan & Morgan
201 N. Franklin Street, 7th Floor
Tampa, FL 33602

Paul C. Whalen
Law Office of Paul C. Whalen, P.C.
768 Plandome Road
Manhasset, NY 11030

For Defendants:

Allyson Himelfarb
Kenneth L. Chernof
Arthur Luk
Stephen Ryck
Arnold & Porter Kaye Scholer LLP
601 Massachusetts Ave. NW
Washington, DC 20001

Hon. Brenda K. Sannes, United States District Judge:

MEMORANDUM-DECISION AND ORDER

I. INTRODUCTION

Plaintiff Ronald Jantzer brings this putative class action against Defendants Elizabethtown Community Hospital (“ECH”) and University of Vermont Health Network, Inc. (“UVM Health”). (Dkt. No. 1). This action arises from a data breach at ECH that allegedly exposed the personally identifiable information (“PII”) of 32,000 ECH patients in October 2018. (*Id.* ¶ 2). Plaintiff brings claims of: (1) negligence, (2) invasion of privacy, (3) breach of implied contract, (4) unjust enrichment, (5) breach of fiduciary duty, (6) breach of confidence, and (7) deceptive, unfair, and unlawful trade acts or practices. (*Id.* ¶¶ 78–173). The complaint invokes federal jurisdiction under the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2). (*Id.* ¶ 11). Presently before the Court is Defendants’ motion to dismiss under Federal Rules of Civil Procedure 12(b)(1) and/or 12(b)(6). (Dkt. No. 13). The parties have filed responsive briefing. (Dkt. Nos. 15, 17). For the reasons below, Defendants’ motion to dismiss under Fed. R. Civ. P. 12(b)(1) is granted.¹

II. FACTS²

UVM Health is Vermont Corporation headquartered in Burlington, Vermont that consists of a “six-hospital and home health & hospice system” located in “Vermont and northern New York.” (Dkt. No. 1, ¶ 10). ECH is a New York corporation headquartered in Elizabethtown, New York and is part of the UVM Health network. (*Id.* ¶ 9).

¹ Given the Court’s finding that Plaintiff lacks standing to bring this action, the Court does not consider Defendants’ motion to dismiss under Rule 12(b)(6).

² The facts are taken from the Complaint, (Dkt. No. 1), and the affidavits and exhibits attached to Defendants’ motion to dismiss. (Dkt. Nos. 13–2–13–4). The Court has considered the affidavits and exhibits because “a defendant is permitted to make a fact-based Rule 12(b)(1) motion.” *Carter v. HealthPort Techs., LLC*, 822 F.3d 47, 57 (2d Cir. 2016).

On October 18, 2018, “ECH discovered that the PII of 32,000 of its patients was compromised as a result of a successful phishing³ attack of one or more of its employees.”⁴ (Dkt. No. 1, ¶ 15). Specifically, “an unauthorized third party acquired credentials that enabled them to remotely access the email account of an ECH employee and thereafter to gain unfettered access to the PII of ECH patients over a period of nine days in October 2018” (the “Data Breach”). (*Id.*). The PII exposed included “names, addresses, Social Security numbers, dates of birth, driver’s license numbers, and medical information such as medical record numbers, dates of service, and summaries of medical services provided.” (*Id.* ¶ 16).

“This Data Breach was a direct result of Defendants’ failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect patient PII.” (*Id.* ¶ 4). Defendants failed to (1) “take adequate and reasonable measures to ensure its data systems were protected,” (2) “disclose that it did not have adequately robust computer systems and security practices,” (3) “take standard and reasonable available steps to prevent the Data Breach,” (4) “monitor and timely detect the Data Breach,” and (5) “provide Plaintiff . . . prompt and accurate notice of the Data Breach.” (*Id.* ¶ 5).

Plaintiff Ronald Jantzer is a patient of ECH. (*Id.* ¶ 8). On December 17, 2018—two months after ECH discovered the data breach—he “received notice from ECH that his PII, along with approximately 32,000 other patients, had been improperly exposed to unauthorized third

³ Phishing “is a method of obtaining personal information using deceptive e-mails and websites” that aims to “trick an e-mail recipient into believing that the message is something they want or need from a legitimate or trustworthy source and to subsequently click on [a] link or download an attachment.” (Dkt. No. 1, ¶ 19). Once this occurs, “the credentials are then used to gain unauthorized access into a system.” (*Id.*).

⁴ The Complaint asserts different dates for when ECH discovered the data breach. Specifically, it asserts that ECH discovered the breach on both October 18, (Dkt. No. 1, ¶ 2), and December 11, 2018. (*Id.* ¶ 15). It also references an online article about the Data Breach, which states that ECH discovered the breach on October 18, 2018, (*Id.* ¶ 15 n.1), and asserts that ECH “waited two months before informing affected patients” in December 2018. (*Id.* ¶ 3). Thus, while the exact date is not relevant to the current motion, the Court will construe the Complaint as alleging ECH became aware of the Data Breach in October 2018.

parties.” (*Id.* ¶¶ 2, 8). The notice informed him that the compromised email account contained some of his “personal information, including [his] name and limited medical information.” (Dkt. No. 13-4, at 2). It also stated that his “Social Security number was not present in the account, and [ECH] do[es] not believe [he] [is] at any financial risk.” (*Id.*).

According to Jennifer Parks, UVM Health’s Network Chief Compliance and Privacy Officer, the compromised email account “did not contain any financial information of [Plaintiff], such as credit or debit card numbers; it did not contain [Plaintiff’s] date of birth; and it did not contain any medical condition(s) for which [Plaintiff] was treated.” (Dkt. No. 13-2, ¶¶ 1, 5). However, the email account “did contain limited information associated primarily with billing” including “information relating to the processing of payment from insurers: date of treatment, information identifying the insurer that provided reimbursement, and payment dates and amounts.” (*Id.* ¶ 6).

Plaintiff “has spent time monitoring and protecting his financial well-being by, among other things, corresponding with the major credit bureaus.” (Dkt. No. 1, ¶ 8). Plaintiff alleges he will continue to spend “significant amounts of time and money in an effort to protect [himself] from the adverse ramifications of the Data Breach and will forever be at a heightened risk of identity theft and fraud.” (*Id.* ¶ 6).

III. STANDARD OF REVIEW

“A case is properly dismissed for lack of subject matter jurisdiction under Rule 12(b)(1) when the district court lacks the statutory or constitutional power to adjudicate it.” *Makarova v. United States*, 201 F.3d 110, 113 (2d Cir. 2000). A lack of standing “may be addressed through a Rule 12(b)(1) motion.” *Lyons v. Litton Loan Servicing LP*, 158 F. Supp. 3d 211, 218 (S.D.N.Y. 2016). “In resolving a motion to dismiss under Rule 12(b)(1), the district court must take all uncontroverted facts in the complaint (or petition) as true, and draw all reasonable inferences in

favor of the party asserting jurisdiction.” *Tandon v. Captain’s Cove Marina of Bridgeport, Inc.*, 752 F.3d 239, 243 (2d Cir. 2014). A defendant may make “a fact-based Rule 12(b)(1) motion, proffering evidence beyond the complaint and its exhibits.” *Nicholas v. Trump*, No. 18-cv-8828, 2020 WL 209274, at *3, 2020 U.S. Dist. LEXIS 6427, at *8 (S.D.N.Y. Jan. 14, 2020) (quoting *Carter*, 822 F.3d at 57). A plaintiff must then “come forward with evidence of their own to controvert that presented by the defendant, or may instead rely on the allegations in the [i]r p]leading if the evidence proffered by the defendant is immaterial because it does not contradict plausible allegations that are themselves sufficient to show standing.” *Id.* (quoting *Katz v. Donna Karan Co., L.L.C.*, 872 F.3d 114, 119 (2d Cir. 2017)).

IV. ANALYSIS

Plaintiff contends he suffered an injury—and thus has standing—for two reasons: (1) “the threa[t] of future harm is sufficiently imminent” and (2) he “has suffered an injury by time spent protecting himself.” (Dkt. No. 15, at 13–16). Defendants argue that “Plaintiff is unable to demonstrate any injury-in-fact” because Plaintiff did not have sufficiently sensitive information stolen in the Data Breach and thus does not face “a risk that is substantial or imminent.” (Dkt. No. 13-1, at 11).

A. General Principles of Standing

“Article III of the Constitution limits federal courts’ jurisdiction to certain ‘Cases’ and ‘Controversies’” and “[o]ne element of the case-or-controversy requirement is that plaintiffs must establish they have standing to sue.” *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 408 (2013) (citation and internal quotation marks omitted). “[T]he irreducible constitutional minimum contains three elements.” *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992). To establish standing, (1) “the plaintiff must have suffered an ‘injury in fact’—an invasion of a legally protected interest,” (2) “there must be a causal connection between the injury and the

conduct complained of,” and (3) “it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.” *Id.* at 560–61 (citations and internal quotation marks omitted). “The party invoking federal jurisdiction bears the burden of establishing these elements.” *Whalen v. Michael Stores Inc.* (“*Whalen I*”), 153 F. Supp. 3d 577, 580 (E.D.N.Y. 2015), *aff’d*, 689 F. App’x 89 (2d Cir. 2017) (quoting *Lujan*, 504 U.S. at 561).

At issue here is the first element—whether Plaintiff suffered an injury in fact that is “(a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical.” *Fero v. Excellus Health Plan, Inc.* (“*Fero I*”), 236 F. Supp. 3d 735, 747 (W.D.N.Y. 2017), *on reconsideration sub nom. Ferro v. Excellus Health Plan, Inc.* (“*Fero II*”), 304 F. Supp. 3d 333 (W.D.N.Y. 2018) (quoting *Lujan*, 504 U.S. at 560). Allegations of future harm “may suffice if the threatened injury is ‘certainly impending,’ or there is a ‘substantial risk’ that the harm will occur.” *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (quoting *Clapper*, 568 U.S. at 414 n.5). However, “[a]llegations of *possible* future injury are not sufficient.” *Clapper*, 568 U.S. at 409 (citation and internal quotation marks omitted). “An injury may include mitigation-related expenses ‘based on a ‘substantial risk’ that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm.’” *Rudolph v. Hudson’s Bay Co.*, No. 18-cv-8472, 2019 WL 2023713, at *3, 2019 U.S. Dist. LEXIS 77665, at *11 (S.D.N.Y. May 7, 2019) (quoting *Clapper*, 568 U.S. at 414 n.5).

In the class action context, “the Court considers the injuries of the named plaintiffs, not unnamed class members.” *Fero I*, 236 F. Supp. 3d at 746. “[I]f none of the named plaintiffs purporting to represent a class establishes the requisite of a case or controversy with the defendants, none may seek relief on behalf of himself or any other members of the class.” *Id.* (quoting *O’Shea v. Littleton*, 414 U.S. 488, 494 (1974)).

B. Risk of Future Harm

Plaintiff contends he has standing because the information stolen was “personal information including names, date of birth, addresses, and some medical information” and this “stolen information is in the hands of bad actors,” creating a “substantial risk of future harm.” (Dkt. No. 15, at 14) (internal quotation marks omitted). Defendants argue that “the undisputed limited nature of the information at issue cannot plausibly result in future identity threat or fraud,” (Dkt. No. 17, at 5), because the “alleged risk is merely speculative and not based on the leakage of information that can be used to inflict harm.” (Dkt. No. 13-1, at 13).

The Second Circuit has not yet addressed the issue of standing for a plaintiff alleging injury based on a data breach. Applying general standing law, district courts have concluded that “[w]hether the risk of identity theft is sufficiently material to create an injury in fact is ‘a question for lower courts to determine in the first instance, on a case- and fact-specific basis.’” *Rudolph*, 2019 WL 2023713, at *4, 2019 U.S. Dist. LEXIS 77665, at *11 (quoting *Sackin v. TransPerfect Glob., Inc.*, 278 F. Supp. 3d 739, 746 (S.D.N.Y. 2017) and *Katz*, 872 F.3d 114, 121 (2d Cir. 2017)); *see also Whalen v. Michaels Stores, Inc.* (“*Whalen II*”), 689 Fed. App’x 89, 90 (2d Cir. 2017) (summary order)); *Fero II*, 304 F. Supp. 3d at 339.

In an unpublished decision, the Second Circuit found that a plaintiff whose credit card information had been stolen failed to allege an injury sufficient to establish standing when she cancelled the credit card without incurring any charges and failed to allege “with any specificity that she had spent time or money monitoring her credit.” *Whalen II*, 689 F. App’x at 90. The Court found that the plaintiff did “not allege how she can plausibly face a threat of future fraud, because her stolen credit card was promptly canceled after the breach and no other personally identifying information—such as her birth date or Social Security number—is alleged to have been stolen.” 689 F. App’x at 90 (citing *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App’x 384,

386 (6th Cir. 2016) (holding that a plaintiff had standing to sue after an intentional data breach of a database including “names, dates of birth, marital statuses, genders, occupations, employers, Social Security numbers, and driver’s license numbers”). This language suggests that the theft of certain personal information, like birth dates and social security numbers, could constitute a substantial risk of harm—and thus an injury in fact. 689 F. App’x at 90. “Other courts have distinguished . . . breaches that disclose personal information that is more susceptible to identity theft” from the breach of payment-card data. *Rudolph*, 2019 WL 2023713, at *5–6, 2019 U.S. Dist. LEXIS 77665, at *15–16 (finding that complaint failed to plausibly allege a substantial risk of future harm from data breach limited to the data on plaintiff’s “now-cancelled” debit card); *see also Sackin*, 278 F. Supp. 3d at 746 (finding “allegations that [d]efendant has provided Plaintiffs’ names, addresses, dates of birth, Social Security numbers and bank account information directly to cyber-criminals creates a risk of identity theft sufficient” to establish standing).

In this case, Plaintiff was informed that his social security number was not included in the data that was stolen. (Dkt. No. 13-4, at 2). While the data breach contained “limited information [of Plaintiff’s] associated primarily with billing,” such as “the date of treatment, information identifying the insurer that provided reimbursement, and payment dates and amounts,” it “did not contain any financial information of [Plaintiff], such as credit or debit cards,” his birth date, or any of his medical conditions. (Dkt. No. 13-2, ¶¶ 1, 5). As Defendant states, “Plaintiff does not contest, controvert, or in any way challenge [Defendants’] showing” regarding what PII of Plaintiff’s was stolen. (Dkt. No. 17, at 5) (emphasis omitted). Thus, the Court must determine whether the theft of Plaintiff’s personal information related to the date and amount of his treatment, and his insurer, creates an imminent risk of identity theft.

The Court finds that it does not, and thus Plaintiff has not alleged the requisite injury in fact necessary for standing. Even assuming that the Second Circuit allowed standing based on an increased risk of future identity theft, “it would be of no help to Plaintiff[] in this case,” *Steven v. Carlos Lopez & Assocs., LLC*, 422 F. Supp. 3d 801, 804 (S.D.N.Y. 2019), because the type of information exposed is not sensitive enough such that identity theft is “certainly impending” or there is a “substantial risk” that it will occur. *Driehaus*, 573 U.S. at 158 (citation omitted). The cases Plaintiff relies on are distinguishable from the instant case because they involved the theft of more sensitive information. (Dkt. No. 15, at 14). See *In re Zappos.com, Inc.*, 888 F.3d 1020, 1023–27 (9th Cir. 2018) (finding the plaintiffs had standing when the data breach included “names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information” and this data “gave hackers the means to commit fraud or identity theft”); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-md-02752, 2017 WL 3727318, at *2, *13, 2017 U.S. Dist. LEXIS 140212, at *31, *62 (N.D. Cal. Aug. 30, 2017) (finding the plaintiffs alleged a “credible threat of real and immediate harm” when the data breached contained information about plaintiffs’ “Yahoo login, country code, recovery e-mail, date of birth, hashed password, cell phone numbers, and zip codes”) (citation and internal quotation marks omitted). Here, the limited nature of information exposed undercuts Plaintiff’s assertion that there is a substantial risk of future harm.⁵ See *Clapper*, 568 U.S. at 409

⁵ Plaintiff argues the fact that “the motive of the hacker was nefarious” and that “a third party did not access the data inadvertently” means that harm is “certainly impending.” (Dkt. No. 15, at 13–15). Whether a third party intentionally targeted sensitive information is a factor courts consider in determining whether the risk of identity theft constitutes an injury-in-fact. See *Steven*, 422 F. Supp. 3d at 806 (finding the plaintiffs failed to establish a substantial risk of harm after their information was exposed because, inter alia, “they do not allege that their data was compromised as a result of a hack or some other criminal act”); *Sackin*, 278 F. Supp. 3d at 746 (holding that the plaintiffs had standing following a data breach that provided hackers with social security numbers, birth dates, and addresses because this information “was provided directly to cybercriminals” whose “most likely and obvious motivation for the hacking is to use Plaintiffs’ PII nefariously or sell it to someone who would”). Nevertheless, despite the fact that “a plaintiff is more likely to establish an injury in fact based on the increased risk of identity theft where the plaintiff has alleged that the third party behind the data breach targeted the plaintiff’s personal information with an intent to use the

(“[A]llegations of *possible* future injury are not sufficient” (citation and internal quotation marks omitted)).

“Those who are entrusted with details about an individual’s health care should guard against even the inadvertent disclosure of that confidential information” and “[t]hose duties were allegedly breached in this case when hackers secured access to confidential health care information through a cyberattack.” *Fero I*, 236 F. Supp. 3d at 742. “Nonetheless, while legal remedies may be pursued by those who were injured, the law only allows for the pursuit of plausible claims—and only by those who have standing based on an alleged legally compensable injury.” *Id.* The Court finds the harm of increased risk of future identity fraud too speculative to support standing in this case.

C. Mitigation Efforts

Plaintiff advances an alternative basis for standing—that he has “suffered an injury by time spent protecting himself.” (Dkt. No. 15, at 15). Defendants contend that “[p]laintiffs are not permitted to use unspecified monitoring to manufacture an injury” because “[m]itigation expenses do not qualify as actual injuries where the harm is not imminent.” (Dkt. No. 17–18 (quoting *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 694 (7th Cir. 2015))).

The Court agrees with Defendants. “In *Clapper*, the Supreme Court held that plaintiffs ‘cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.’” *Fero I*, 236 F. Supp. 3d at 754 (quoting *Clapper*, 568 U.S. at 416)). See, e.g., *In re SuperValu, Inc.*, 870 F.3d 763, 771 (8th Cir. 2017) (“Because plaintiffs have not alleged a substantial risk of future identity theft, the time

information fraudulently,” *In re 21st Century Oncology Customer Data Sec. Breach Litig.*, 380 F. Supp. 3d 1243, 1252 (M.D. Fla. 2019), Plaintiff cites no caselaw to support the notion that standing is conferred when data is intentionally hacked even if the data stolen does not pose a material risk of identity theft, as in this case.

they spent protecting themselves against this speculative threat cannot create an injury.”); *Steven*, 422 F. Supp. 3d at 807 (rejecting the plaintiffs’ contention that they had standing based on the “time and money spent monitoring or changing their financial information and accounts”). In this case, Plaintiff’s allegation that “he has spent time monitoring and protecting his financial well-being, by, among other things, corresponding with the major credit bureaus,” (Dkt. No. 1, ¶ 8), is thus not sufficient to confer standing. *See Whalen II*, 689 F. App’x at 91 (stating that the plaintiff “pleaded no specifics about any time or effort that she herself has spent monitoring her credit” and so “she alleged no injury that would satisfy the constitutional standing requirements of Article III”). This case is unlike *Rudolph*, where the plaintiff’s specific allegations, detailing the time and expense she had incurred in obtaining a replacement debit card, established a concrete injury sufficient for Article III standing. *Rudolph*, 2019 WL 2023713, at *7, 2019 U.S. Dist. LEXIS 77665, at *21–23.

V. CONCLUSION


For these reasons, it is hereby

ORDERED that Defendants’ motion to dismiss for lack of standing (Dkt. No. 13) is **GRANTED**; and it is further

ORDERED that the Complaint (Dkt. No. 1) is **DISMISSED without prejudice** under Fed. R. Civ. P. 12(b)(1) for lack of subject matter jurisdiction.

IT IS SO ORDERED.

Dated: May 12, 2020
Syracuse, New York


Brenda K. Sannes
U.S. District Judge